

Some Nonexistence Results for Strong External Difference Families Using Character Theory

William J. Martin¹ and Douglas R. Stinson²

¹Department of Mathematical Sciences, Worcester Polytechnic Institute, 100 Institute Road, Worcester, MA 01609, USA

²David R. Cheriton School of Computer Science, University of Waterloo, Waterloo, Ontario, N2L 3G1, Canada

October 21, 2016

Abstract

In this paper, we study the existence of (v, m, k, λ) -strong external difference families (SEDFs). We use character-theoretic techniques to show that no SEDF exists when v is prime, $k > 1$ and $m > 2$. In the case where v is the product of two distinct odd primes, some necessary conditions are derived, which can be used to rule out certain parameter sets. Further, we show that, when $m = 3$ or 4 and $v > m$, a (v, m, k, λ) -SEDF does not exist. Finally, we prove that there is no SEDF in any elementary abelian 2-group.

1 Introduction

Motivated by applications to *algebraic manipulation detection codes* (or AMD codes) [1, 2, 3], Paterson and Stinson introduced *strong external difference families* (or SEDFs) in [9]. SEDFs are closely related to but stronger than *difference systems of sets* [7] and *external difference families* (or EDFs) [8]. In [9], it was noted that optimal AMD codes can be obtained from EDFs, whereas optimal strong AMD codes can be obtained from SEDFs. See [9] for a discussion of these and related structures and how they relate to AMD codes. In this paper, we focus on SEDFs, the existence of which is an interesting mathematical problem in its own right, independent of any applications to AMD codes.

We recall the definition of SEDFs from [9, Defn. 2.5] now. Let G be a finite abelian group of order v (written multiplicatively) with identity element $1 \in G$. For parameters k, λ, m such that

$$k^2(m-1) = \lambda(v-1) \tag{1}$$

we seek (pairwise disjoint) subsets $D_1, \dots, D_m \subseteq G$ with $|D_j| = k$ ($1 \leq j \leq m$) satisfying

$$\sum_{\ell \neq j} D_j D_\ell^{-1} = \lambda(G-1) \tag{2}$$

for each $1 \leq j \leq m$, where the above equation holds in the group algebra $\mathbb{C}[G]$. For convenience, we capture the remaining defining conditions here:

$$D_1, D_2, \dots, D_m \subset G, \quad |D_j| = k \quad \forall j, \quad |G| = v \tag{3}$$

where G is a finite abelian group. A collection (D_1, \dots, D_m) satisfying conditions (2) and (3) is denoted as a (v, m, k, λ) -SEDF.

Let \mathcal{D} denote the union of all the sets D_j : in group algebra notation,

$$\mathcal{D} = \sum_{j=1}^m D_j.$$

With this, Equation (2) becomes

$$D_j \mathcal{D}^{-1} - D_j D_j^{-1} = \lambda(G - 1). \quad (4)$$

Two infinite classes of SEDFs are known, when $k = 1$ and $m = 2$. These were shown in [9].

Example 1.1. Let $G = (\mathbb{Z}_{k^2+1}, +)$, $D_1 = \{0, 1, \dots, k-1\}$ and $D_2 = \{k, 2k, \dots, k^2\}$. This is a $(k^2+1, 2, k, 1)$ -SEDF.

Example 1.2. Let $G = (\mathbb{Z}_v, +)$ and $D_i = \{i\}$ for $0 \leq i \leq v-1$. This is a $(v, v, 1, 1)$ -SEDF.

The following theorem is also proved in [9].

Theorem 1.1. [9] There does not exist a $(v, m, k, 1)$ -SEDF with $m \geq 3$ and $k > 1$.

In [9], the authors ask if there are any additional parameters for which SEDFs exist. Some necessary conditions for the existence of SEDFs have recently been obtained by Huczynska and Paterson [4] using combinatorial techniques. Their results include a substantially complete treatment of the case $\lambda = 2$. In this paper, we apply linear characters of G to both sides of the equation (4) to rule out the existence of SEDFs in groups of prime order. We also give some partial results (i.e., necessary conditions) for (abelian) groups whose order v is the product of two distinct primes, as well as a non-existence result for SEDFs in elementary abelian 2-groups.

We now state and prove a simple numerical result, concerning parameters for SEDFs, that we will use later.

Lemma 1.2. There does not exist a (v, m, k, λ) -SEDF with $v = mk$ and $k > 1$.

Proof. From (1), we have $k^2(m-1) = \lambda(km-1)$. Clearly, $\gcd(k, km-1) = 1$, so it follows that $k^2 \mid \lambda$. Thus, $\lambda = tk^2$ for some positive integer t , and hence $m-1 = t(km-1)$. This shows that $k = t = 1$. \square

2 Some facts about characters

We briefly review some basic facts about characters of finite abelian groups. These can be found, for example, in [6].

For a finite abelian group G , there are exactly $v = |G|$ distinct homomorphisms from G to the multiplicative group of complex numbers. First consider a cyclic group $G \cong (\mathbb{Z}_v, +)$. Let ω denote a primitive v^{th} root of unity, e.g., $\omega = e^{2\pi i/v}$. For $0 \leq a < v$, take $\chi_a : G \rightarrow \mathbb{C}^*$ via

$$\chi_a(b) = \omega^{ab}.$$

For $a = 0$, we have the trivial character, which we will denote by $\mathbb{1}$. Every finite abelian group G is isomorphic to a direct product of finite cyclic groups and their characters can be pieced together to give $|G|$ distinct characters of G . If $\phi : G \rightarrow \mathbb{Z}_{m_1} \times \dots \times \mathbb{Z}_{m_r}$ is an isomorphism and $\chi^{(j)}$ is a character of \mathbb{Z}_{m_j} ($1 \leq j \leq r$), then, for $\phi(g) = (b_1, \dots, b_r)$,

$$\psi(g) = \chi^{(1)}(b_1) \chi^{(2)}(b_2) \dots \chi^{(r)}(b_r)$$

is a character for G . When G is abelian, the product of characters $(\chi\psi)(g) = \chi(g)\psi(g)$ is again a character and, provided G is finite, this gives us a group of characters isomorphic to G . So we can label the $|G|$ distinct characters $\{\chi_a \mid a \in G\}$.

These characters χ, ψ, \dots satisfy the following “orthogonality” relations: $\chi_a(b) = \chi_b(a)$ and

$$\sum_{b \in G} \overline{\chi(b)} \psi(b) = \begin{cases} v & \text{if } \chi = \psi \\ 0 & \text{otherwise.} \end{cases}$$

So, for any non-principal character (i.e., $\chi \neq \mathbb{1}$), we have $\sum_b \chi(b) = 0$. Likewise $\sum_\chi \chi(b) = 0$ unless $b = 1$ in G , in which case the sum equals v .

Each χ extends to an algebra homomorphism from the group algebra $\mathbb{C}[G]$ to \mathbb{C} . Since the “Fourier matrix” whose columns are the v characters is invertible, this provides us a bijection from $\mathbb{C}[G]$ to the vector space \mathbb{C}^v . Under this bijection, we have 0 mapping to 0, $1 \in G$ mapping to the all ones vector in \mathbb{C}^v , and the element

$$G = \sum_{a \in G} a$$

mapping to the vector $(v, 0, \dots, 0)$. So $G - 1$ maps to $(v - 1, -1, \dots, -1)$.

Since G is finite, every value $\chi(g)$ lies on the unit circle in \mathbb{C} . Clearly, $\chi(g^{-1}) = \overline{\chi(g)}$. For $S \subseteq G$, we abbreviate the group algebra element $\sum_{a \in S} a$ to simply “ S ”. We then easily see that, for $S^{-1} := \sum_{a \in S} a^{-1}$, we have

$$\chi(S^{-1}) = \overline{\chi(S)}.$$

We remark that most of our discussion below never relies on the particular structure of the group G . However, we do assume that G is an abelian group of order v , not necessarily cyclic.

3 Applying characters to prove results about SEDFs

If we apply the trivial character to Equation (4), we obtain Equation (1). Suppose, on the other hand, that χ is a non-principal character. Applying χ to Equation (4), we obtain

$$\chi(D_j) \overline{\chi(\mathcal{D})} - \chi(D_j) \overline{\chi(D_j)} = -\lambda. \quad (5)$$

Since the right-hand side is non-zero, we immediately have $\chi(D_j) \neq 0$ for all j . Here are some more basic observations:

Lemma 3.1. (a) For any character χ of G ,

$$\chi(\mathcal{D}) = \sum_{j=1}^m \chi(D_j) \quad (6)$$

(b) For any character χ of G ,

$$\chi(D_j) \neq 0 \quad \forall 1 \leq j \leq m, \quad \forall \chi \neq \mathbb{1}. \quad (7)$$

(c) If χ is a non-principal character such that $\chi(\mathcal{D}) = 0$, then, for all $1 \leq j \leq m$,

$$\chi(D_j) \overline{\chi(D_j)} = \lambda.$$

(d) $\mathbb{1}(\mathcal{D}) = |\mathcal{D}| = mk$ and, except when $\mathcal{D} = G$ or $\mathcal{D} = \emptyset$, there is at least one non-principal character χ satisfying $\chi(\mathcal{D}) \neq 0$.

Proof. Part (a) follows from linearity. Parts (b) and (c) follow immediately from equation (5). For part (d), we make use of the fact that the Fourier matrix is invertible, which implies that $\mathbb{C}[G]$ is in bijective correspondence with \mathbb{C}^v . For each complex number z , we already know one preimage of $(z, 0, \dots, 0)$; so if $\mathbf{g} \in \mathbb{C}[G]$ with $\chi(\mathcal{D}) = (z, 0, \dots, 0)$, then $\mathbf{g} = \frac{z}{v}G$. \square

We now conjugate Equation (5) and obtain

$$\chi(\mathcal{D}) = \frac{|\chi(D_j)|^2 - \lambda}{\overline{\chi(D_j)}} \quad \forall j. \quad (8)$$

Note that, when $k = 1$, the assumption that \mathcal{D} is a set (and not a multiset) forces $\mathcal{D} = G$ and we have $\chi(\mathcal{D}) = 0$ for every non-trivial character χ of G . So our analysis does not apply in the case $k = 1$.

Lemma 3.2. *Let $\chi \neq \mathbb{1}$. If $\chi(\mathcal{D}) \neq 0$, then there exist nonzero real numbers $\alpha_1, \dots, \alpha_m$ such that $\chi(D_j) = \alpha_j \chi(\mathcal{D})$ for $j = 1, \dots, m$.*

Proof. We know

$$\overline{\chi(D_j)}^{-1} = \frac{\chi(D_j)}{|\chi(D_j)|^2},$$

so we obtain

$$\chi(\mathcal{D}) = \left(\frac{|\chi(D_j)|^2 - \lambda}{|\chi(D_j)|^2} \right) \chi(D_j)$$

from equation (8). $\chi(\mathcal{D})$ and $\chi(D_j)$ are both nonzero, so

$$\alpha_j = \frac{|\chi(D_j)|^2}{|\chi(D_j)|^2 - \lambda}$$

is nonzero. Further, α_j is clearly a real number. □

So let's fix $\chi \neq \mathbb{1}$ and, assuming $\chi(\mathcal{D}) \neq 0$, denote $\chi(\mathcal{D}) = X$ and $\chi(D_j) = x_j = \alpha_j X$. We obtain a system of quadratic equations from (5) which gives us restrictions on the values α_j . For $m = 2$, this simply tells us $\alpha_1 \alpha_2 = -\lambda/X\bar{X}$ and rules nothing out. However, for $m \geq 3$, we obtain some useful information. We first consider the case $m = 3$.

Theorem 3.3. *There does not exist a $(v, 3, k, \lambda)$ -SEDF for any $v > 3$.*

Proof. First, since $v > 3$, it follows from Lemma 1.2 that we cannot have $\mathcal{D} = G$. Hence, from Lemma 3.1(d), there is a non-principal character χ such that $\chi(\mathcal{D}) \neq 0$. Now, from (5), we have

$$\begin{array}{rclcl} x_1 \bar{x}_2 & + & x_1 \bar{x}_3 & & = & -\lambda \\ x_2 \bar{x}_1 & & & + & x_2 \bar{x}_3 & = & -\lambda \\ & & x_3 \bar{x}_1 & + & x_3 \bar{x}_2 & = & -\lambda. \end{array}$$

We conjugate the second equation and subtract it from the first to obtain $x_1 \bar{x}_3 = \bar{x}_2 x_3$. In the same manner, we find $x_1 \bar{x}_2 = x_2 \bar{x}_3 = x_3 \bar{x}_1$. Hence, $\alpha_1 \alpha_2 = \alpha_2 \alpha_3 = \alpha_3 \alpha_1$. This forces $\alpha_1 = \alpha_2 = \alpha_3$ since all α_i 's are nonzero. But now we have a contradiction: our first equation becomes

$$\alpha_1^2 X \bar{X} + \alpha_1^2 X \bar{X} = -\lambda$$

with the lefthand side nonnegative and the righthand side negative. This shows $m = 3$ cannot occur. □

For larger values of m , (5) gives us m equations

$$\sum_{\ell \neq j} x_j \bar{x}_\ell = -\lambda \quad (9)$$

($j = 1, \dots, m$). For any distinct indices r and s , we find

$$x_r \bar{x}_s + \sum_{\ell \neq r, s} x_r \bar{x}_\ell = -\lambda$$

and, after conjugation,

$$x_r \bar{x}_s + \sum_{\ell \neq r, s} \bar{x}_s x_\ell = -\lambda$$

so that

$$\sum_{\ell \neq r, s} x_r \bar{x}_\ell = \sum_{\ell \neq r, s} \bar{x}_s x_\ell. \quad (10)$$

Therefore, we have

$$\sum_{\ell \neq r, s} \alpha_r \alpha_\ell X \bar{X} = \sum_{\ell \neq r, s} \alpha_s \alpha_\ell X \bar{X}.$$

Recall we are assuming $X \neq 0$. So we obtain

$$\alpha_r \left(\sum_{\ell \neq r, s} \alpha_\ell \right) = \alpha_s \left(\sum_{\ell \neq r, s} \alpha_\ell \right). \quad (11)$$

Lemma 3.4. *For $m > 3$, there can be only two possible values for α_j ($1 \leq j \leq m$) when $X \neq 0$.*

Proof. Consider three distinct indices r, s, t . If $\alpha_r \neq \alpha_s$, then Equation (11) gives

$$\alpha_t = - \sum_{\ell \neq r, s, t} \alpha_\ell.$$

Likewise, if $\alpha_r \neq \alpha_t$, then

$$\alpha_s = - \sum_{\ell \neq r, s, t} \alpha_\ell,$$

i.e., $\alpha_s = \alpha_t$. □

3.1 Highly uneven—or even—splits cannot occur

We first introduce some notation. We assume that $m > 3$, and

$$\{\alpha_1, \dots, \alpha_m\} \subseteq \{\alpha, \beta\}$$

with $\alpha_j = \alpha$ for exactly A values of j and $\alpha_j = \beta$ for exactly B values of j . Without loss of generality, we assume $0 \leq A \leq B$, and we know that $A + B = m$. The ordered pair (A, B) will be called the *split* of $(\alpha_1, \dots, \alpha_m)$.

Lemma 3.5. *Let $m > 3$ and $\chi \neq 1$ with $X \neq 0$. Then the split of $(\alpha_1, \dots, \alpha_m)$ cannot be $(0, m)$, $(1, m-1)$ or $(m/2, m/2)$.*

Proof. We have

$$\alpha A + \beta B = 1 \quad (12)$$

since $\sum_j x_j = X$, and

$$\alpha_j \left(\sum_{\ell \neq j} \alpha_\ell \right) = -\frac{\lambda}{X \bar{X}} \quad (13)$$

from Equation (9).

If $A = 0$ (i.e., all the α_j 's are equal), then $\beta = 1/m$ by (12). But this gives a positive value for the left-hand side of (13) while the right-hand side is negative, a contradiction.

Next, if $A = 1$ and $B = m-1$, we employ (11) to find $\alpha((m-2)\beta) = \beta((m-2)\beta)$. Since $\beta \neq 0$ by Lemma 3.2, this gives $\alpha = \beta$, which is the case we just discussed.

Finally, if m is even and $A = B$, then (11) with $\alpha_r = \alpha$ and $\alpha_s = \beta$ gives $\alpha + \beta = 0$. But this is impossible since, if $A = B = m/2$, we must have $\alpha + \beta = 2/m$ from (12). □

For small values of m , the three cases handled in Lemma 3.5 cover all or most of the possible splits.

Theorem 3.6. *There does not exist a $(v, 4, k, \lambda)$ -SEDF for any $v > 4$.*

Proof. First, since $v > 4$, it follows from Lemma 1.2 that we cannot have $\mathcal{D} = G$. Hence, from Lemma 3.1(d), there is a non-principal character χ such that $\chi(\mathcal{D}) \neq 0$. The result then follows from Lemma 3.5. \square

The following also follows from Lemma 3.5.

Theorem 3.7. *Suppose there is a (v, m, k, λ) -SEDF with $k > 1$.*

- (a) *If $m = 5$, the split for any $\chi \neq \mathbb{1}$ with $\chi(\mathcal{D}) \neq 0$ must be $(A, B) = (2, 3)$.*
- (b) *If $m = 6$, the split for any $\chi \neq \mathbb{1}$ with $\chi(\mathcal{D}) \neq 0$ must be $(A, B) = (2, 4)$. \square*

Example 3.1. *We analyze the case $m = 5$. Restrict to some $\chi \neq \mathbb{1}$ with $X := \chi(\mathcal{D}) \neq 0$. From Theorem 3.7, without loss of generality, there exist real numbers α and β with*

$$\alpha_1 = \alpha_2 = \alpha \neq \beta = \alpha_3 = \alpha_4 = \alpha_5.$$

Equation (11) with $r = 1$, $s = 3$ gives $\alpha + 2\beta = 0$. Combining this with (12), we find

$$\alpha = 2, \quad \beta = -1.$$

So

$$\chi(D_r + D_s + D_t) = 0$$

whenever $r \in \{1, 2\}$ and $s, t \in \{3, 4, 5\}$. This gives us $2|X|^2 = \lambda$ using Equation (8), which seems perfectly valid at this point. We have six different proper subsets of G over which the character χ sums to zero. This happens (for some choices of χ) when the subset is a coset of a proper subgroup of G , so perhaps this is possible.

3.2 The case of prime v

In this section, we make use of some results of Lam and Leung [5]. We first summarize the material we need from their paper in a single theorem.

Theorem 3.8. [5] *Let G be a finite cyclic group of order v , where v has prime power factorization $v = p_1^{r_1} \cdots p_s^{r_s}$ and let χ be a non-principal character of G . Let $\mathcal{E} \in \mathbb{Z}[G]$, say*

$$\mathcal{E} = \sum_{g \in G} n_g g.$$

- (a) *If $\chi(\mathcal{E}) = 0$, then there exist nonnegative integers k_1, \dots, k_s such that*

$$\sum_{g \in G} n_g = k_1 p_1 + \cdots + k_s p_s.$$

- (b) *If v is prime and $\mathcal{E} \subseteq G$ with $\chi(\mathcal{E}) = 0$, then $\mathcal{E} = \emptyset$ or $\mathcal{E} = G$.*
- (c) *If $v = pq$, where p and q are distinct primes, and $\mathcal{E} \subseteq G$ with $\chi(\mathcal{E}) = 0$, then there exists a nonnegative integer k such that $|\mathcal{E}| = kp$ or $|\mathcal{E}| = kq$. Further, \mathcal{E} is expressible as a disjoint union of cosets of some proper subgroup H of G (where $|H| = p$ or $|H| = q$).*

The last statement (part (c)) is not directly given in the paper of Lam and Leung. But it follows immediately from their results. They prove in [5] that, if $\mathcal{E} = \sum_{g \in G} n_g g$ is a multiset (i.e., all $n_g \geq 0$), then $\sum_g n_g$ is expressible as $kp + k'q$ for non-negative integers k and k' . But, by the Chinese Remainder Theorem, we cannot have both k and k' nonzero when \mathcal{E} is simply a subset of G (because any coset of a subgroup of order p intersects any coset of a subgroup of order q , as in the following example).

Example 3.2. Consider $G = \mathbb{Z}_{77}$. Then any multiset \mathcal{E} with $\chi(\mathcal{E}) = 0$ is expressible as a union (counting multiplicities) of cosets of $7G$ and cosets of $11G$. But any coset $a + 7G$ has non-trivial intersection with any coset $b + 11G$, because the system of congruences

$$\begin{aligned} x &\equiv a \pmod{7} \\ x &\equiv b \pmod{11} \end{aligned}$$

has a unique solution modulo 77.

Here is the main theorem of this section, which completely handles the case where the group G has prime order.

Theorem 3.9. *If v is prime, $k > 1$ and $m > 2$, then there does not exist a (v, m, k, λ) -SEDF.*

Proof. We can assume $m \geq 5$ in view of Theorems 3.3 and 3.6. Select $\chi \neq \mathbf{1}$ with $\chi(\mathcal{D}) \neq 0$. By Lemma 3.5, we have two distinct real numbers α, β such that $\alpha_j \in \{\alpha, \beta\}$ for $1 \leq j \leq m$, with each value occurring at least twice. Choose r and s with $\alpha_r = \alpha$ and $\alpha_s = \beta$. Then Equation (11) forces

$$\chi \left(\sum_{\ell \neq r, s} D_\ell \right) = 0. \quad (14)$$

However, the set

$$\bigcup_{\ell \neq r, s} D_\ell$$

has cardinality $k(m-2)$ which lies strictly between 0 and v . This contradicts Theorem 3.8(b). \square

3.3 The case $v = pq$, where p and q are distinct primes

Suppose $v = pq$, where p and q are distinct primes. We assume $k > 1$ and $m > 2$. We have the following:

$$k^2(m-1) = \lambda(v-1) \quad (15)$$

$$v = pq \quad (16)$$

$$k(m-2) \equiv 0 \pmod{p} \quad (17)$$

$$km < v. \quad (18)$$

Note that (15) is just (1). The congruence (17) follows from (14) and Theorem 3.8(c), where without loss of generality we can assume that (17) holds for the prime divisor p (if not, we can interchange p and q). Finally, (18) is just Lemma 1.1.

From (17), there are two possible cases to consider:

case 1: $p \mid k$, or

case 2: $p \mid (m-2)$.

We now derive some necessary conditions that must hold if we are in case 1. Suppose $p \mid k$; then $k = sp$, where s is a positive integer. From (15), we have $p^2 \mid \lambda$, so let $\lambda = tp^2$, where t is a positive integer. Then (15) becomes

$$s^2(m-1) = t(v-1).$$

Now, $spm = km < v = pq$, so $sm < q$. Further,

$$t(v-1) = s^2(m-1) < s^2m \leq qs,$$

so we have

$$s > \frac{t(v-1)}{q}.$$

Then,

$$k = sp > \frac{pt(v-1)}{q} \geq \frac{p(v-1)}{q}.$$

Now, if $k > v/5$, then $m < 5$, which is impossible by Theorems 3.3 and 3.6. Therefore,

$$\frac{p}{q} \leq \frac{v}{5(v-1)} = \frac{1}{5} + \frac{1}{5(v-1)}. \quad (19)$$

This inequality (19) can sometimes be used to rule out certain parameter situations.

Example 3.3. Suppose $v = 77 = 7 \times 11$, $k > 1$ and $m > 2$. The inequality (19) does not hold, so we conclude that $m \equiv 2 \pmod{7}$ or $m \equiv 2 \pmod{11}$ (since case 1 does not hold, case 2 must apply). Thus, $m \geq 9$. Since $km < v$, we see that $k \leq 8$.

Now consider equation (15), which gives $k^2(m-1) = 76\lambda$. This implies that $19 \mid k$ or $19 \mid (m-1)$. If $19 \mid k$, then $k \geq 19$, which is impossible because $k \leq 8$. Therefore, $19 \mid (m-1)$. However, as mentioned above, we also have $m \equiv 2 \pmod{7}$ or $m \equiv 2 \pmod{11}$. If $m \equiv 2 \pmod{7}$, then the system of congruences has the solution $m \equiv 58 \pmod{153}$ so $m \geq 58$. Then $k = 1$, which contradicts the assumption $k > 1$. If $m \equiv 2 \pmod{11}$, then $m \equiv 134 \pmod{209}$ so $m \geq 134$. This is clearly impossible. We conclude there is no $(77, m, k, \lambda)$ -SEDF with $k > 1$ and $m > 2$.

However, there certainly are parameter sets that satisfy all the necessary conditions given above.

Example 3.4. Suppose $p = 7$, $q = 31$, $v = pq = 217$, $m = 9$, $k = 9$ and $\lambda = 3$. Here $m \equiv 2 \pmod{p}$, $k^2(m-1) = 648 = \lambda(v-1)$ and $km = 81 < v$. So the above arguments do not rule out the existence of a $(217, 9, 9, 3)$ -SEDF.

3.4 Elementary abelian 2-groups

Suppose $G \cong \mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2$ is an elementary abelian group of order 2^n . Then all characters are real-valued functions (taking only values ± 1) and equation (5) becomes

$$x_j X - x_j^2 = -\lambda.$$

So there can be at most two values of x_j , namely $\frac{1}{2}(X \pm \sqrt{X^2 + 4\lambda})$. Let us suppose that one of these values, say $\frac{1}{2}(X + \sqrt{X^2 + 4\lambda})$, occurs t times and the other one occurs $m - t$ times. From Lemma 3.5, we know that $2 \leq t \leq m - 2$. So, in equation (10), we may contrast $x_r = x_s = \frac{1}{2}(X + \sqrt{X^2 + 4\lambda})$ with $x_r = x_s = \frac{1}{2}(X - \sqrt{X^2 + 4\lambda})$. The two equations become

$$\begin{aligned} (t-2) \left(\frac{X + \sqrt{X^2 + 4\lambda}}{2} \right) + (m-t) \left(\frac{X - \sqrt{X^2 + 4\lambda}}{2} \right) &= 0 \\ t \left(\frac{X + \sqrt{X^2 + 4\lambda}}{2} \right) + (m-t-2) \left(\frac{X - \sqrt{X^2 + 4\lambda}}{2} \right) &= 0. \end{aligned}$$

These can be written as

$$\begin{aligned} (m-2) \frac{X}{2} + \frac{2t-m-2}{2} \sqrt{X^2 + 4\lambda} &= 0 \\ (m-2) \frac{X}{2} + \frac{2t-m+2}{2} \sqrt{X^2 + 4\lambda} &= 0. \end{aligned}$$

But then we have $2\sqrt{X^2 + 4\lambda} = 0$, which is a contradiction. So we have proven the following.

Theorem 3.10. If $v = 2^n$, then there does not exist any (v, m, k, λ) -SEDF in the elementary abelian 2-group of order v .

4 Conclusion

Character-theoretic techniques have been a powerful tool in the study of “classical” difference sets for many years. So it is not surprising that this approach is useful in investigating strong external difference families. So far, the only known examples of SEDFs are those in two “trivial” infinite classes mentioned in [9]. Our paper has ruled out the existence of SEDFs for other classes of parameters. It remains to be seen if there are any examples of SEDFs other than the two aforementioned infinite classes.

One interesting case is when $m = 2$. Our techniques do not say anything about this case, and there are numerous parameter sets with $m = 2$ that satisfy the necessary conditions. Further, one of the two known infinite families of SEDFs has $m = 2$.

Acknowledgements

WJM thanks the Cheriton School of Computer Science (University of Waterloo) for hosting him while the initial work on this project was done. He is also grateful to Jim Davis and the University of Richmond for hosting a helpful workshop related to this subject.

Research of DRS is supported by an NSERC discovery grant.

References

- [1] R. Cramer, Y. Dodis, S. Fehr, C. Padró, D. Wichs. Detection of algebraic manipulation with applications to robust secret sharing and fuzzy extractors. *Lecture Notes in Computer Science* **4965** (2008), 471–488 (Eurocrypt 2008).
- [2] R. Cramer, S. Fehr and C. Padró. Algebraic manipulation detection codes. *Science China Mathematics* **56** (2013), 1349–1358.
- [3] R. Cramer, C. Padró and C. Xing. Optimal algebraic manipulation detection codes in the constant-error model. *Lecture Notes in Computer Science* **9014** (2015), 481–501 (TCC 2015).
- [4] S. Huczynska and M.B. Paterson. Existence and non-existence results for strong external difference families. Preprint.
- [5] T.Y. Lam and K.H. Leung. On vanishing sums of roots of unity. *J. Algebra* **224** (2000), 91–109.
- [6] W. Ledermann. *Introduction to Group Characters, 2nd Ed.*, Cambridge University Press, 1987.
- [7] V.I. Levenshtein. One method of constructing quasilinear codes providing synchronization in the presence of errors. *Problems of Information Transmission* **7** (1971), 215–222.
- [8] W. Ogata, K. Kurosawa, D.R. Stinson and H. Saido. New combinatorial designs and their applications to authentication codes and secret sharing schemes. *Discrete Mathematics* **279** (2004), 383–405.
- [9] M.B. Paterson and D.R. Stinson. Combinatorial characterizations of algebraic manipulation detection codes involving generalized difference families. *Discrete Mathematics* **339** (2016), 2891–2906.